IBSEC-CSS-M-20
24 February 1970

COMPUTER SECURITY SUBCOMMITTEE

OF THE

UNITED STATES INTELLIGENCE BOARD

SECURITY COMMITTEE

Minutes of Meeting
Held at CIA Headquarters
Langley, Virginia
24 February 1970

1. The twentieth meeting of the Computer Security Subcommittee was held on 24 February 1970 between 1330 and 1615 hours in Room 4E-64, CIA Headquarters. In attendance were:

[redacted] STAT
Mr. Richard F. Kitterman, State Member
[redacted] STAT
Mr. Thomas A. Eccleston, Army Member
Mr. Robert B. Cameron, Navy Member
Lt. Col. Charles V. Burns, Air Force Member
[redacted] STAT
Mr. Conrad S. Banner, FBI Alternate
Mr. Raymond J. Brady, AEC Member
[redacted] STAT
Mr. Alexander S. Chodakowski, State
[redacted] STAT

Group 1
Excluded from automatic
downgrading and
declassification

[redacted] STAT

Mr. William S. Donaldson, Air Force

[redacted] STAT

2. The security level of the meeting was announced as Top Secret COMINT.

3. Approval of Minutes: The minutes of the 9 February 1970 meeting were approved without change.

4. Update Briefing on DIA Analyst Support and Research System (ANSRS): At the beginning of the instant meeting Mr. [redacted] of DIAMS presented a briefing on the progress of the development of ANSRS since the earlier presentation to the Subcommittee at the beginning of 1969. STAT

5. A significant portion of this update briefing consisted of a description of the security features built into the ANSRS operation; these features fall into six general categories:

a) Physical security;
b) Personnel security;
c) Technical security;
d) Administrative safeguards;
e) User procedural safeguards;
f) Computer center procedural safeguards.

6. [redacted] briefing evoked numerous questions from individual Subcommittee members concerning specific details of the various security features mentioned. These questions were fielded by [redacted] with assistance from [redacted] and [redacted] The entire briefing and question period served as a forum for meaningful discussion of the problem of securing a modern time-sharing computer system with remote access capabilities. The Chairman on behalf of the Subcommittee expressed appreciation for [redacted] effort. STAT STAT STAT STAT

S-E-C-R-E-T

7. Subsequently at the meeting [redacted] who was STAT in charge of a security test and evaluation of ANSRS, provided a brief description of this which was conducted in the second quarter of calendar year 1969. This security test attempted to measure the technical features of the system as well as the procedural control features. Data was collected in the test period through machine generated statistics, tests conducted by security, technical, and user personnel, and through questionaires completed by system users. A conclusion was reached on the basis of these security tests which provided a favorable analysis on the efficacy of ANSRS security. [redacted] noted, however, that its results were STAT pertinent and relevant to the system as it existed in the test period; he is not familiar with the development of the system after that date.

8. Security Requirements for Multilevel Operations: The Chairman made reference to the fact that although individual agency submissions for the most part have been received for preparation of a Subcommittee paper outlining key security features useful in the development of multilevel operations, consolidation of these submissions has been delayed. He requested that the Subcommittee at the task team level begin to address this task as soon as possible.

9. In addition, the requirement is foreseen that the Subcommittee paper include an outline of fundamental requirements which will permit a remote terminal time-shared system to operate in a multilevel mode, as long as the environment is benign. Making reference to his earlier proposal of specific requirements toward this end, the Chairman asked for further discussion of this issue at the instant and at future meetings. Consideration at the instant meeting was predicated upon a request from DIA in view of the presence of ANSRS personnel.

10. The Chairman also noted that the responsibility for developing such fundamental requirements was clearly within the purview of the Subcommittee under the terms of reference outlined in its charter coupled with the recommendation in the Fall of 1969 to the DCI from the PFIAB. The Chairman noted that at the 18 February IHC meeting he had indicated that the Subcommittee was addressing

the multilevel problem with a view toward recommendation for USIB implementation fundamental system security features which would permit multilevel operation in a system where all persons having access thereto hold a minimum of a Top Secret clearance. The Chairman also noted that he had briefed the COINS Software Security Panel on the problem and outlined the proposed minimum standards discussed at earlier Computer Security Subcommittee meetings. In both cases the proposal was generally well received.

11. The AEC member commented that although such minimum standards might be applied to the multilevel operations at AEC headquarters, it would be extremely difficult to implement them at contractor locations. [ ] further indicated his belief that audit trail information should be maintained on data classified SECRET and above, but not on unclassified and Confidential material; this opinion is based on the fact that no strict control of such data is maintained now in the manual arena. STAT

12. [ ] expressed his view with reference to the password capability feature that the number of key words used in a given system should be limited; he believed that the use of multiple passwords is cumbersome and difficult to administer since individuals find it impossible to remember more than one or two. As an alternative he suggested the utilization of access controls which would tie a specific user's authenticator with the degree of access that person has to the system. DIA was requested to submit its comments in writing concerning security requirements for multilevel operations. In this way its views could be used as direct input for the Subcommittee paper being discussed. STAT

13. Continued discussion of this item is foreseen on future agendas.

14. Security Labeling Standards: Members were reminded that the deadline had arrived for agency submissions with reference to the Security Labeling Standards Project. He noted that the FBI and an interim DIA paper were the only inputs received to date. He requested that all others be forwarded by the next Subcommittee meeting.

15. Computer Threat Analysis: The Chairman advised that he had provided the Security Committee at its 17 February meeting with an interim report on this task. The Security Committee was told that the Subcommittee felt that any analysis of the postulated threat in the computer environment was not necessary. The Chair-

25X1

these cases could not be reported to the Committee at this time, but the Chairman is making appropriate inquiry with the agencies concerned.

16. The Chairman advised the Subcommittee of his intention to provide a written report to the Security Committee on the matter of analyzing the threat in the computer environment. This report will be prepared as soon as the agencies controlling the suppressed cases are contacted for guidance.

17. System Testing and Evaluation: The Chairman reported to the Subcommittee that he had attended the 18 February IHC meeting at the request of its CIA member in view of the planned discussion on that date of a DIA proposal that the IHC sponsor a security test and evaluation of ANSRS with a view toward the accreditation of that system to operate in a multilevel environment. Members were advised that the problem of system security testing and evaluation is by no means limited to the DIA proposal,, since individually all USIB agencies have a requirement for determining the security effectiveness of their systems. The Chairman suggested a need for the Subcommittee to discuss the development of basic criteria and general guidelines for the conduct of such tests. In addition the establishment of minimum standards for the multilevel operation of computer systems would greatly facilitate the conduct of system testing and evaluation. No prolonged discussion of this item was had at the instant meeting, but it is foreseen that the Subcommittee will be addressing this issue in further detail as time continues.

18. Degaussing Study: The Chairman requested that members of the task team assigned to handle the degaussing study draft preparation begin their efforts as soon as possible.

19. Training Course Task Effort: The Chairman of the Training Course Task Team was requested to submit a detailed progress report at the next Subcommittee meeting.

20. DSB Report: The Chairman announced that he had been informed during the past week that the report of the Defense Science Board Computer Security Task Force had been submitted to the DSB in early February and was now in the process of being published. Further, he indicated his understanding that an unclassified version of the report is expected to receive wide dissemination.

21. Possible Disk Degaussing Device: The Chairman reported that he had recently heard of a disk degaussing device being marketed by a local computer distributor. He had contacted the distributor's representative who confirmed the availability of a disk degausser; the firm's representative is obtaining details on the instrument and is to report to the Chairman in the near future.

22. The next Subcommittee meeting was scheduled for 0930 hours on 9 March 1970.

STAT

Chairman
Computer Security Subcommittee